ABSTRACT

Methods and apparatus detecting attempts to obtain IP addresses by faking a MAC address in a data portion of an IP address request message are described. In accordance with the present invention, rather than use standard address allocation protocols, e.g., ARP, the DNS DCHP contacts the requesting edge router via a private secure network. The MAC address received in the address request is compared to the MAC addresses stored in the edge routers port/MAC address resolution table. If the MAC address received in the request message cannot be found in the edge router's table which was created from the MAC address included in the message's header, a fraudulent attempt to obtain a MAC address is declared. The fraudulent attempt to obtain an IP address can be reported and steps taken to identify the perpetrator of the fraud.